Secureworks®

SERVICE DESCRIPTION

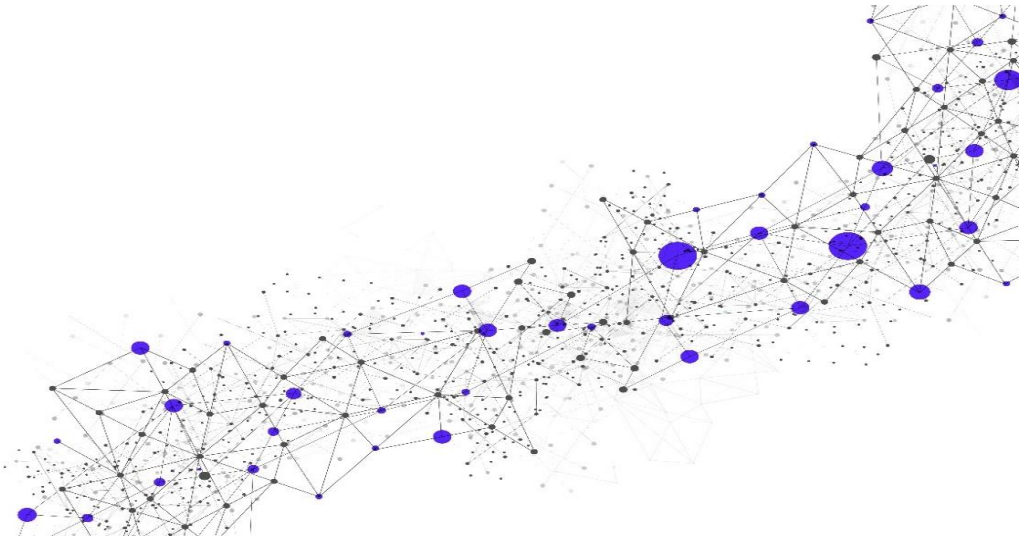
Incident Management Retainer Services*

Release Date

February 06, 2024

Version

10.0



www.secureworks.com

Global Headquarters
1 Concourse Pkwy NE #500
Atlanta, GA 30328
Phone: +1 877 838 7947
Email: info@secureworks.com
Additional office locations: https://www.secureworks.com/about/offices

This Service Description only applies to IMR Service purchased by Customer prior to July 31, 2020.

* This SD is ***only*** for purchases of the following, as specified in Customer's Service Order:
  - Retainer: Incident Management: Promotional
  - Incident Management Retainer SMB ONLY
  - Incident Management Retainer

Table of Contents

1 Service Introduction

This Service Description ("**SD**") describes the Incident Management Retainer Services ("**Service**"). This SD only applies to Service ***purchased by Customer prior to July 31, 2020***. All capitalized words and phrases shall have the meanings set forth herein, as defined in the Glossary, or within the Secureworks-applicable agreement, such as the Customer Relationship Agreement for direct or indirect purchases (individually referenced herein as "**CRA**"), that is incorporated herein by reference. For avoidance of doubt, the CRA available at www.secureworks.com/eula (or at www.secureworks.jp/eula-jp for Customers located in Japan) applies to Customer's purchases through an authorized Secureworks' reseller.

The Secureworks® Incident Management ("**IM**" or "**Incident Management**") Retainer ("**IM Retainer**") Services (the "Service") provides a full spectrum of use cases and capability maturity for IM Retainer Services that are described in this SD. All Services are available in the English language only.

Customer may select to apply the IM Retainer to one or more of the Service components set forth below. Upon request by Customer and upon completion of a particular Service component, Secureworks will notify Customer of the remaining IM Retainer balance. The duration of the Service is agreed upon by the parties as set forth in the Service Order Term (as defined below). Each Service component performed under this IM Retainer will vary during the Term, based upon Customer needs and availability of hours.

The Service components are summarized in the table below.

Service Option	Components
Emergency Incident Response Services	• Emergency Incident Response Services • Digital Forensic Analysis Services • Malware Analysis and Reverse Engineering Services

Proactive Incident Response Services	• Targeted Threat Hunting Assessment
	• Incident Response Readiness Assessment
	• Incident Response Plan Development
	• Incident Response Plan Review
	• Incident Response Workshops
	  ○ First Responders Training
	  ○ Threat Briefings
	  ○ Open Source Information Briefings
	• Incident Response Exercises
	  ○ Tabletops
	  ○ Functional Exercises

1.1 Deliverables

Secureworks will work with Customer to determine the appropriate deliverables, delivery method, and cadence.

Service	Report	Delivery Schedule	Delivery Method
Incident Response Engagements	Status Updates	Agreed-upon intervals	Agreed-upon methods
	Final	Upon completion of each Engagement	Secure Email, Client Portal, Secure File Sharing

1.1.1 Status Updates

Status Updates may be verbal or written and may include:

- Summary of completed activities
- Issues requiring attention
- Planning for the next work effort period

1.1.2 Final Report

Final Report may include:

- Executive summary, outlining key findings and recommendations
- Methods, detailed findings, narratives and recommendations
- Attachments providing relevant details and supporting data

Secureworks will issue a Final Report to Customer-designated point of contact within three (3) weeks of completing the active phases of the Engagement. Customer shall then have three (3) weeks from Secureworks delivery of the Final Report to provide comments. Should Customer provide comments, the Final Report shall be deemed complete upon the earlier of the date which (1) Secureworks provides responses to these comments or (2) Secureworks delivers a revised Final Report. If no comments are received from Customer before the expiration of the review period, or upon Customer's written acceptance of the Report, the Final Report will be deemed complete and referred to as the "Completed Final Report".

1.2 Customer Obligations

Customer acknowledges that Secureworks' ability to perform the Services is contingent upon the following:

- Customer personnel are scheduled and available to assist as required for the Service(s).
- Customer will have obtained consent and authorization from the applicable third party, in form and substance satisfactory to Secureworks, to permit Secureworks to provide the Service if Customer does not own network resources such as IP addresses, Hosts, facilities or web applications.
- For on-site activities, Customer will provide a suitable workspace for Secureworks personnel, and necessary access to systems, network, and devices.
- Replies to all requests will be prompt and in accordance with the delivery dates established between the parties.
- Customer's scheduled interruptions and maintenance intervals allow adequate time for Secureworks to perform the Service.
- Customer will promptly inform Customer personnel and third parties of Secureworks testing activities as needed, to prevent disruption to Secureworks business and performance of the Service (e.g., takedown requests, ISP deny list).

- Customer will provide to Secureworks all required information (key personnel contact information, credentials, etc.) at least two (2) weeks before an Engagement for a Proactive Service, or prior to on-site arrival for Emergency Incident Response.

2 Service Details

2.1 Incident Management Retainer

2.1.1 Initiation of an Engagement

Customer shall initiate a request for IR Services through the Incident Response Hotline or Secureworks Client Portal, and Secureworks will draft an "Engagement Request for Incident Management Services" document upon receipt of this request. Customer and IR personnel will determine the appropriate course of action based on the estimated work effort required.

2.1.2 Pre-Engagement

The Service provides Customer a wide range of Proactive Incident Response Services and Emergency Incident Response Services. Customer may apply Retained Hours against one or more services described within this Appendix.

Upon receipt of Customer-executed Purchase Order, Secureworks will:

- Distribute contact information for engaging Secureworks; contact information includes the Incident Response Hotline, IR Resource Coordinator, and IR senior managers
- Clarify escalation channels and verify Customer contact information
- Coordinate Retained Hour utilization notifications, and facilitate meetings to scope any immediate IR Service needs

2.1.2.1 Incident Response Hotline

Secureworks will distribute several regional, toll-free, Incident Response Hotline numbers to be used by Customer when there is a confirmed or suspected cyber incident. A Secureworks representative will receive the call, and engage the Secureworks Incident Response team to contact Customer and determine the appropriate next steps.

2.1.2.2 Engagement Approval Process

After Customer submits a request for Incident Response Services, the Secureworks Incident Response team members will gather Customer requirements. The course of action for each Engagement will be mutually agreed upon by Customer and Secureworks on a case-by-case basis.

2.2 Emergency Incident Response Services

Emergency Incident Response Services can be provided remotely or on-site.

The activities to be performed may include, but are not limited to:

- Incident support and coordination
- Digital media handling guidance and support
- Deployment support of host-based, network-based, and log analysis technologies
- Network testing services
- Incident Response analysis for on-premises and cloud infrastructure

  - Host-based
  - Network-based
  - Malicious code
  - Logs
  - Threat intelligence analysis
- Remediation planning guidance

Interim Reports may include:

- Engagement status reporting and action item tracking
- Engagement findings and recommendations reporting
- Engagement support with Customer or through Customer with other third parties

Final Report may include:

- Executive summary, outlining key findings and recommendations
- Methods, detailed findings, narratives, and recommendations
- Attachments providing relevant details and supporting data

2.2.1 Digital Forensic Analysis Services

As part of Emergency Incident Response Services, Secureworks may acquire and analyze a variety of formats for forensic analysis and data recovery, including but not limited to:

- Disk drives
- RAID systems
- Portable storage drives
- Mobile devices
- Network packet captures
- Cleartext log files

2.2.2 Malware Analysis and Reverse Engineering Services

As part of Emergency Incident Response Services, Secureworks may perform static, dynamic, and reverse engineering analysis to assist in understanding, the function of Customer-supplied files.

Secureworks will provide analysis results, to include cyber threat intelligence based on correlation across Secureworks datasets, and will advise on mitigation actions to reduce the impact of the sample on Customer infrastructure.

2.3 Proactive Incident Response Services

2.3.1 Threat Hunting Assessment

Secureworks will perform a Threat Hunting Assessment in Customer’s environment, reviewing traces that persist in Endpoint Sensors, Network Sensors, and retained logs to identify indicators and behaviors of compromise activity. The activities to be performed may include, but are not limited to:

- Digital media handling guidance and support
- Deployment support of host-based, network-based, and log analysis technologies

- Targeted threat hunting analysis for on-premises and cloud infrastructure
  - Host-based
  - Network-based
  - Malicious code
  - Logs
  - Threat intelligence analysis

At the close of the Engagement, Customer will receive a Final Report.

In the event that previous or ongoing compromise activity is discovered, Secureworks can provide Customer with Emergency Incident Response services to the extent mutually defined by Customer and Secureworks.

2.3.2 Incident Response Readiness Assessment

The IR Readiness Assessment is intended to provide broad visibility into the state of Customer IR capability. Secureworks facilitates activities to identify strengths and weaknesses in existing processes and procedures, resulting in detailed recommendations for focused improvement. The Engagement requires involvement from both technical and non-technical Customer resources to ensure a comprehensive understanding of the current state of Customer IR capability.

At the close of the Engagement, Customer will receive a Final Report that provides executive-level overview material of the results of the assessment, in order to describe to leaders the state of their readiness to respond to an incident and detail areas for improvement.

This Information Briefing will take the form of a Final Report that contains a point-in-time snapshot of internet information available about Customer or the identified individuals. Analysis focuses on identifying areas where security controls can limit the impact of the information, and highlight the areas of greatest risk if the data was used maliciously.

2.3.3 Incident Response Plan Development

Secureworks will assist with developing Cyber Incident Response Plan materials. At the strategic level, Secureworks will assist with IR plan development, security policy integration, capability development, and governance. From a tactical standpoint, Secureworks will help define IR workflows, roles, responsibilities, and detection and response processes specific to Customer.

Secureworks will request documentation that supports the effort to understand Customer's current posture and practices to draft IR materials tailored to Customer. The documentation requested may consist of items such as process diagrams, policies, procedures, guidelines, and any other pertinent information necessary to help Secureworks to understand current practices and regulatory requirements.

Facilitated workshops and interviews may also be conducted with key stakeholders to gather a deeper understanding of overall requirements, critical business requirements, and existing response capabilities.

The Engagement requires commitment and participation from Customer representatives by actively participating in the development process, providing information in a timely manner, and reviewing drafted content to confirm the material is suitable for Customer.

Secureworks will create a Final Report that includes an Incident Response Plan and Process materials incorporating any previously available content that may be available.

2.3.4 Incident Response Plan Review

Secureworks will conduct a detailed review of the existing Cyber Incident Response Plan ("**CIRP**") to assess the current IR posture and practices. The IR Plan Review may also include interviews with key stakeholders.

Secureworks will provide Customer with a Final Report that includes prioritized risk findings and detailed recommendations to improve Incident Response practices. The documentation review may consist of the following:

- Process diagrams
- Policies, procedures, and guidelines
- Other information to help Secureworks understand current practices and regulatory requirements

2.3.5 Incident Response Workshops

2.3.5.1 First Responders Training

Secureworks will facilitate Customer IR First Responders Training with specific topics customized to improve Customer's IR capabilities that may include:

- IR process fundamentals
- Digital media handling and Chain of Custody
- Volatile data collection
- Forensic imaging techniques

The Engagement must be conducted on-site at a Customer-designated location. Completion of the training class is the equivalent of the Completed Final Report described in Deliverables, and signifies the completion of the Engagement.

2.3.5.2 Threat Briefings

Conference calls, online workshops, or on-site workshops can be arranged to review topics of interest that fall within the domains of Incident Response and Threat Intelligence. These include but are not limited to:

- Lessons learned from previous incidents
- Current state of Customer IR capabilities
- Current threats and adversary tactics, techniques, and procedures
- Assistance with developing materials for Customer-internal meetings

Completion of the Briefing is the equivalent of the Completed Final Report described in Deliverables, and signifies the completion of the Engagement.

2.3.5.3 Open Source Information Briefings

Secureworks will create an Open Source Information Briefing about Customer, which is an aggregation and analysis of information available through Open Source Intelligence ("**OSINT**") sources.

Secureworks personnel leverage OSINT to identify files, proprietary information, and metadata that are used for targeting individuals, or that could be used to compromise the security posture, financial assets, or brand reputation of Customer. Secureworks personnel also use information from social media sites, public filings, data found in underground sites, and Secureworks' proprietary data sets to show the level of exposure to malicious data mining.

2.3.6 Incident Response Exercises

2.3.6.1 Tabletops

An IR Tabletop Exercise assembles key stakeholders, and walks through a scripted incident. The exercise facilitator releases information in a controlled manner that will guide the exercise, while each stakeholder describes their response as if it were a real incident. IR tabletop exercises are an efficient way to familiarize staff with IR practices, and they proactively test existing response capabilities, including the validation of roles, responsibilities, coordination, and decision making.

At the close of the Engagement, Customer will receive an after-action Final Report that summarizes the event activities with risk-prioritized findings and recommendations to improve IR practices.

2.3.6.2 Functional Exercises

After Customer is confident in its ability to react well during an IR Tabletop Exercise, IR Functional Exercises allow Customer personnel to validate their technical readiness performing their actual hands-on duties in a simulated manner. Secureworks adds technical artifacts to a tabletop-like exercise that Customer must analyze to understand the scenario playing-out.

IR Functional Exercises vary in complexity and scope, ranging from validating specific aspects of a plan, to full-scale exercises that address all plan elements. Secureworks can coordinate overt, covert, and full-spectrum IR functional exercises.

2.3.6.2.1 Overt

Customer participants perform each step of the plan as if it were a real incident, using any processes, tools, and techniques at their disposal. Participants perform actual response activities but are aware that it is an exercise.

2.3.6.2.2 Covert

Only Customer's point of contact is aware that the Engagement is an exercise. Typically, only Customers with mature response capabilities can successfully perform covert Engagements due to the complexity of preparing and coordinating the exercise.

2.3.6.2.3 Full-spectrum

The Engagement builds on prior functional exercises by leveraging the Secureworks red team acting as an attacker, testing the breadth of Customer capabilities. By carrying out activities to simulate real-world adversarial tactics, the actual operational capability of IR people, process, and technology can be evaluated in real time.

At the close of the Engagement, Customer will receive a Final Report that summarizes the event activities with risk-prioritized findings and recommendations to improve IR practices.

2.4 Out of Scope

Secureworks reserves the right to decline requests which:

- Are beyond the scope of the Services as defined herein
- Are beyond the capability of Secureworks to deliver within contracted service levels
- Might violate legal or regulatory requirements

3 Terms and Conditions

3.1 Service Fees

Fees for this service and the minimum hours required are defined in an associated Quote or Service Order. Until the Service Order is fully executed by both parties, Customer understands that the fees proposed are only valid for 90 days from the date received.

3.1.1 Billing for Services

- Single year Service Fees are 100% billable upon Service Order execution.
- Multi-year Service Fees for Year 1, if applicable, are billable upon Service Order execution.
- Multi-year Service Fees for Year 2, if applicable, are billable upon the first anniversary of Service Order execution.
- Multi-year Service Fees for Year 3, if applicable, are billable upon the second anniversary of Service Order execution.
- Secureworks will keep Customer informed of the balance of Customer's Retained Hours.
- For a single year Service Order, any unused Retained Hours at the end of the Service Order Term will be forfeited.
- For a multi-year Service Order, any unused Retained Hours at the end of each year of the Service Order Term will be forfeited.
- See also the Service-specific Addendum incorporated herein by reference at https://www.secureworks.com/legal/product-terms, as updated from time to time (the "Product Terms Page") for additional information about invoice commencement. Provisions related to the term of the Service and payment terms within the Product Terms Page shall not apply to Customer's consumption of Services in case of purchases through a Secureworks' reseller but instead shall be subject to Customer's agreement with its reseller.

3.1.2 Additional Hours

- Additional blocks of hours may be purchased in advance of or upon exhaustion of contracted hours at the contracted rate referenced in the Services Fees Section via e-mail authorization from Customer.
- Requests for additional hours must be sent through e-mail from Customer to irservices@secureworks.com. Customer acknowledges and agrees that receipt of such e-mail will be from a Customer representative authorized to commit Customer to the purchase of additional hours and email notification is binding upon Customer.
- Customer acknowledges and agrees that if Purchase Orders (P.O.s) are required for the transaction with Secureworks to extend or add to the originally purchased service(s), then an updated P.O. will be issued to Secureworks for the extended/added service(s) specified in the authorizing email within seven (7) calendar days from the date of the acknowledged receipt of the email by Secureworks. If an updated P.O. is not received within 7 calendar days, then Secureworks may terminate the service(s) and/or Engagement as applicable and notwithstanding the foregoing, Customer acknowledges and agrees that it remains responsible for any additional work performed by Secureworks until such P.O. is received.

3.1.3 Retained Hours

- Each service request will be scoped, and a minimum number of Committed Hours will be established prior to Engagement start.
- Customer may terminate an Engagement by providing 24-hour advance notice to stop all work against the Purchase Order and/or Service Order. Committed Hours will be forfeited if Engagement is terminated prior to exhaustion of those hours.
- Notice for termination of Engagement must be sent by email to irservices@secureworks.com.
- Consumed hours will be calculated in quarter-hour increments.
- All Retained Hours and Committed Hours are non-refundable and non-transferable for other Secureworks services. Any Retained Hours and Committed Hours specified for any contract year that are not used within such contract year shall be forfeited.

3.2 Expenses

Customer agrees to reimburse Secureworks, directly or indirectly (in case of purchases through an authorized reseller), for all reasonable and actual expenses incurred in conjunction with delivery of the Service.

These expenses include, but are not limited to:

- Travel fees related to transportation, meals and lodging to perform the Services, including travel to Customer locations
- Media storage, specific equipment, or licensing necessary for forensic work
- Monthly fees for other purchased infrastructure to support service delivery (e.g., public cloud computing services) may apply, should Customer and Secureworks agree that usage is necessary to complete the Engagement.

3.3 Incident Management Retainer Service Level Agreement ("SLA")

These SLAs shall apply to the Services described herein, subject to the following terms, conditions, and limitations:

Service	SLA Description	Credit
Proactive Incident Response Services	• Requests for Proactive Incident Response Services submitted via the Incident Response Hotline will be acknowledged by the Secureworks Incident Response team within one (1) business day. • Service requests submitted outside of the Incident Response Hotline will be addressed on a best-effort basis and are outside the scope of this SLA.	5 Retained Hours for each business day that the SLA is not met
Emergency Incident Response Services	• Emergency Incident Response Service submitted via the Incident Response Hotline will be acknowledged by the Secureworks Incident Response team within four (4) hours. • Secureworks will commence work on Emergency Incident Response Engagement within 24 hours of agreement on scope. • Secureworks will have personnel on-site within 36 hours of	5 Retained Hours for each business day that the SLA is not met

Service	SLA Description	Credit
	agreement on scope for locations within Australia, EU member states, Japan, the Schengen Area and the USA, ("On-site Response Supported Locations"). • For locations outside of "On-site Response Supported Locations," Secureworks will have personnel in transit within 48 hours of agreement on scope, unless Secureworks deems those locations unsafe. For locations deemed by Secureworks as unsafe, Secureworks solely reserves the right to limit travel to those locations or to require a security escort at additional customer expense. Customer will be notified at the time services are requested if additional security is required, and Customer will be required to authorize the additional expense before travel is arranged. • Service requests submitted outside of the Incident Response Hotline will be addressed on a best-effort basis and are outside the scope of this SLA. • Emergency Incident Response services declared within fourteen (14) calendar days from the P.O Effective Date will be addressed on a best-effort basis and are outside the scope of this SLA. • Customer shall receive Emergency Incident Response Service Final Report within three (3) weeks from the completion of the mutually defined Service work effort.	

4 Service Delivery

4.1 Delivery Coordination

Secureworks will provide coordination for the services in scope with appropriate communication and updates to the stakeholder community. The coordinator will oversee logistics for people, processes, and tools as well as timeline and meeting facilitation.

The scope of delivery coordination includes:

- Develop delivery timeline with Customer and with Secureworks resources
- Work with Customer to identify and address issues or concerns that impact service delivery
- Periodic, high-level updates on progress
- Confirm delivery and procure project sign-off

4.2 Scheduling

4.2.1 Proactive Incident Response Services

Customer should request Proactive Incident Response Services using the Incident Response Hotline and Client Portal that are available 24 hours a day, 7 days a week.

Proactive Incident Response Services outlined within this Service Order require a minimum of four (4) weeks advance notification to schedule, and must be scheduled with sufficient time to complete the activity within the Service Order Term.

If Customer requests multiple Proactive Incident Response Services simultaneously, Secureworks will schedule the first request as described within this section, with following requests scheduled as best-effort based on resource availability.

4.2.2 Emergency Incident Response Services

For Emergency Incident Response Services, Customers should request Services using the Incident Response Hotline and Client Portal that are available 24 hours a day, 7 days a week.

4.2.3 Cancellations

Once scheduling of any on-site work at Customer facility has been mutually agreed to, any changes by Customer to the on-site work within two (2) weeks of the on-site work to be performed will incur a $2,000 re-scheduling fee. This re-scheduling fee does not apply to work that does not require travel by Secureworks.

4.2.4 Delivery

For locations deemed by Secureworks as unsafe, Secureworks solely reserves the right to limit travel to those locations or to require a security escort at additional customer expense. Customer will be notified at the time services are requested if additional security is required, and Customer will be required to authorize the additional expense before travel is arranged.

5 Service Order Term

The term of this Service Order shall commence on the Service Order Effective Date and terminate on the date which is one (1), two (2) or, three (3) years thereafter, based on your Service Order (the "**Service Order Term**").

The term of the Services for the Incident Management Retainer shall commence on the Service Order Effective Date and terminate on the earlier to occur of (i) the Service Order Term, or (ii) the completion of any outstanding time and materials billing (the "**Services Term**").

To the extent that Customer authorizes work effort for an Engagement, and such work effort extends beyond the Service Order Term or Services Term, the Service Order Term and Services Term shall be extended to the completion of such continued work effort through the date of the Completed Final Report (the "Extended Term"). During such Extended Term, the terms and conditions of this Service Order and the MSA shall be in full force and effect.

6 Additional Terms

6.1 On-site Services

Notwithstanding Secureworks' employees' placement at Customer's location(s), Secureworks retains the right to control the work of such employees. For international travel, on-site Services may require additional documentation, such as visas, visitor invitations, and related documentation, which may affect timing of the Services and reimbursable expenses.

6.2 Security Services

Customer acknowledges that the Security Services described herein could possibly result in service interruptions or degradation regarding Customer's systems and accepts those risks and consequences. Customer hereby consents and authorizes Secureworks to provide any or all of the Security Services with respect to Customer's systems. Customer further acknowledges that it is Customer's responsibility to restore network computer systems to a secure configuration after Secureworks completes testing.

6.3 Record Retention

Secureworks will retain a copy of the Customer Reports and supporting Customer Data in accordance with Secureworks' record retention policy.

Unless Customer gives Secureworks written notice to the contrary prior thereto and subject to the provisions of the applicable CRA and DPA, all Customer Data collected during the Services and stored by Secureworks will be deleted within thirty (30) days from issuance of the final Customer Report. If Customer or its authorized agent requests that Secureworks retain Customer Data for longer than its standard retention policy, Customer shall pay Secureworks' costs and expenses associated with the extended retention and storage of such Customer Data. Notwithstanding the foregoing, Secureworks shall be entitled to retain Customer Data as necessary to comply with its own legal, regulatory, judicial, audit, or internal compliance requirements.

6.4 Compliance Services

Customer understands that, although Secureworks' Services may discuss or relate to legal issues, Secureworks does not provide legal advice or services, none of such Services shall be deemed, construed as or constitute legal advice and that Customer is ultimately responsible for retaining its own legal counsel to provide legal advice. Furthermore, any written summaries or reports provided by Secureworks in connection with any Services shall not be deemed to be legal opinions and may not and should not be relied upon as proof, evidence or any guarantee or assurance as to Customer legal or regulatory compliance.

6.5 Post-Engagement Activities

Subject to any applicable legal or regulatory requirements, thirty (30) days after the completed Engagement, Secureworks will commence with the appropriate media sanitization and/or destruction procedures of the Customer acquired images, hard drives or other media obtained by Secureworks in the performance of the Services hereunder (the "**Engagement Media**"), unless prior to such commencement, Customer has specified in writing to Secureworks any special requirements for Secureworks to return such Engagement Media (at Customer's sole expense). Upon Customer's request, Secureworks will provide options for the transfer to Customer of Engagement Media and the related costs thereto. If so requested, Secureworks will provide a confirmation letter to Customer addressing completion and scope of these post-Engagement activities, in Secureworks' standard form. Unless agreed to otherwise by the parties, and subject to any applicable legal or regulatory requirements, Secureworks shall, in its sole discretion, dispose of the Engagement Media on or after the Engagement conclusion and only maintain a copy of the completed Engagement-specific Deliverables.

6.6 Legal Proceedings

If Customer knows or has reason to believe that Secureworks or its employees performing Services under this Service have or will become subject to any order or process of a court, administrative agency or governmental proceeding (e.g., subpoena to provide testimony or documents, search warrant, or discovery request), which will require Secureworks or such employees to respond to such order or process and/or to testify at such proceeding, Customer will (i) promptly notify Secureworks, unless otherwise prohibited by such order or process, (ii) use commercially reasonable efforts to reduce the burdens associated with the response, and (iii) reimburse Secureworks for (a) its employees' time spent as to such response, (b) its reasonable and actual attorneys' fees as to such response, and (c) its reasonable and actual travel expenses incurred as to such response. Nothing in this paragraph shall apply to any legal actions or proceedings between Customer and Secureworks as to the Services.

6.7 Endpoint Assessment

Unless otherwise agreed upon in writing, if a software agent has been deployed as part of an Engagement, within thirty (30) days following the date of the Completed Final Report (the "**Thirty Day Period**"), Customer shall uninstall any and all copies of the software agent used for the Engagement. During the Thirty Day Period, (i) Customer shall not use the software agent, and (ii) the license and use restrictions that apply to the software agent remain in effect notwithstanding the expiration of termination of the Service. Customer will install Secureworks' proprietary software agent if Endpoint Assessment Services are in scope. Customer (i) will use the Endpoint Assessment software agent for its internal security purposes, and (ii) will not, for itself, any Affiliate of Customer or any third party: (a) decipher, decompile, disassemble, reconstruct, translate, reverse engineer, or discover any source code of the software agent; and (b) will not remove any language or designation indicating the confidential nature thereof or the proprietary rights of Secureworks from the software agent. Customer will uninstall the software agent as described in this Service.